**A Comment in Support of the Proposal**

**RM-11699**

**Encryption of Amateur Radio Communications**

I support the proposal for **strictly limited** use of encryption in the Amateur Radio service, subject to additional regulatory restrictions. The agencies we serve are increasingly loathe to permit the transmission of their sensitive traffic via unprotected means. Legal authority to use encryption in these circumstances would facilitate disaster response and might very well save lives. However, I believe it is important to strictly circumscribe the content that can be legally obscured and to require that no other information or communication be hidden from public view.

An important facet of amateur radio support during emergencies is the party-line nature of the communication. All parties monitoring the channel are kept informed about the general state of affairs within a disaster area. This type of information dissemination is critical to our served agencies and would be damaged by the indiscriminate use of encryption. Therefore, *the use of encryption during an emergency or training exercise should be limited to only the sensitive or critical content that requires such protection*.

Technical issues related to implementing limited encryption should be left to the amateur community. This type of experimentation and development is what the service is best at providing. A protocol for transmitting the headers and unobscured portion of a message in the clear, switching to a protected section, and then switching back could easily be designed within the amateur community. These technical issues can be worked out within the context of the amateur radio service as the implications of this new capability become clear and new behaviors are learned.

Some commenters claim that technical issues surrounding the deployment of encryption are reasons to forbid its use. For example, what key exchange protocol should be used? Public-key exchange between two parties would result in a flexible and ad-hoc method of truly securing a communication, but would eliminate the party-line advantage. Shared-key techniques would permit party-line communication, but the securing of keying material within a loosely organized emergency environment is likely impractical. These matters are irrelevant to the regulatory provisioning of encryption in service of the public good. I would like to again suggest that *strictly limiting the portion of any communication that can be encrypted would mitigate any damage to the shared and public nature of the amateur radio service* that the use of encryption might introduce. Under such regulation, any of a variety of strong techniques could be used for private

party-to-party data exchange while requiring that most traffic be sent unobscured. Successful technical approaches will survive in the field and unsuccessful techniques discarded, without requiring any subsequent regulatory changes due to such evolution.

Some commenters are claiming that the MARS or some other radio service are more appropriate for transmission of protected traffic. I disagree. Amateur radio practitioners spend a great deal of money and time establishing and maintaining a reliable communications infrastructure in order to serve their localities. Practiced behaviors are learned by operators within an area. Equipment suited to local obstacles such as terrain or interference are used to meet local needs. It is not reasonable or likely even possible to attempt to suddenly move all of this infrastructure and protocol over to new frequencies just for the transmission of a protected component of an amateur radio message. Without the established infrastructure and protocols, communication may not even be possible – this is the point of provisioning the infrastructure and conducting ongoing training exercises in the first place.

Regulation would be helpful in establishing a fundamental design objective and legal requirement that **only critical or sensitive portions of a communication may be encrypted and all other uses forbidden**. The self-policing nature of the amateur radio service would then be used to detect infringement, just as it is for detection and reporting of any noncompliant transmissions today. The presence of clear regulatory guidelines indicating what portion can be protected and what cannot would mean that the use of encryption does not obscure the identities of transmitting parties nor the general purpose of the communication. Most commenters objecting to the use of encryption seem to believe that all portions of a communication must be protected, while the reality is far different. A simple, succinct regulatory guideline limiting the scope of encryptable content to only sensitive or critical information would help to ensure that both sensitive data and the public nature of the amateur radio service are protected.

It is my opinion that *with such a strong limitation in place*, any damage to the public good from the introduction of encryption into the amateur radio service would be minimized. The relative increase in our ability to serve the public by the exchange of sensitive or critical information more than offsets any danger (real or perceived) from permitting its use during emergencies and training exercises in such a limited form.

William F. Alexander, Jr. K6WFA
2013-06-28